27

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-304808

(43)Date of publication of application : 18.10.2002

(51)Int.Cl. G11B 20/10
G06F 1/00
G06F 12/14
G11B 7/004
G11B 7/007
G11B 20/12

(21)Application number : 2002-018467

(22)Date of filing : 28.01.2002

(71)Applicant : EASTMAN KODAK CO

(72)Inventor : BARNARD JAMES A
INCHALIK MICHAEL A
HA BRUCE L

(30)Priority

Priority number : 2001 772149 Priority date : 29.01.2001 Priority country : US

(54) COPY PROTECTION USING MULTIPLE SECURITY LEVELS ON A PROGRAMMABLE CD-ROM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a method for making copy protection that cannot be subverted by a bit-for-bit copying scheme on standard CD-writers.

SOLUTION: This invention provides a copy-protected optical diskincluding a pre-formed identification number (ID) in the ATIP(Absolute Time In Pre- groove) signal and the subcode which is impressed upon the optical disk and a number of other optical disks during optical disk manufacturea unique identification number for the optical disk which was written on the optical disk after it is manufacturedand an encrypted program written onto the optical disk wherein the encryption of such program is based upon the performed ID and the unique ID and includes two or more selectable security levels.

CLAIMS

[Claim(s)]
[Claim 1]An identification number (ID) which is the optical disk by which the copy protection was carried outis an identification number (ID) in a :aATIP signal and a sub-code formed beforehandand is described at said optical disk and other optical disks at the time of optical disk manufacture and which was formed beforehand;
b) Enciphered program; which was written in peculiar identification number; and the c aforementioned optical disk about said optical disk written in said optical disk after being manufactured is comprisedAn optical disk performing encryption of the program based on said ID formed beforehand and said peculiar IDand having two or a selectable security level beyond it and by which the copy protection was carried out.
[Claim 2]The optical disk according to claim 1 having said formed ID which was described at the main channel data streamand which was formed beforehand and by which the copy protection was carried out.
[Claim 3]A master disc which includes an identification number (ID) which is the method of carrying out the copy protection of the information recorded on an optical diskand was recorded on a :aATIP signal and a sub-codeand which was formed beforehand is formedA step which forms two or more optical disks which have the same ID as said master disc;
b) Step; which writes in a program enciphered by step; and the c aforementioned optical disk which write peculiar ID about an optical disk in an optical disk is comprisedA methodwherein encryption of the program is performed based on said ID formed beforehand and said peculiar identification number.
[Claim 4]A method according to claim 3wherein said ID formed beforehand is recorded on said data stream.
[Claim 5]A method according to claim 3wherein said ID formed beforehand is recorded on specific information of said ATIP signal including the greatest start about said diskand start information of derivation.
[Claim 6]A method of comprising a step of which encryption of an enciphered program is canceled using a step which reads said ID formed beforehand and said peculiar ID from said disksaid ID formed beforehandand said peculiar ID according to claim 3.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to the copy protection to the information recorded on the disk recorded a compact disc and optically [others].
[0002]
[Description of the Prior Art]The consumer-buying layer of the optical disk containing an audioan imagesoftwareor data produced billions of dol commercial scene. It spread that the appearance of the optical recording medium of a low

price and driver which can be set copied the contents without authority in recent years. In order to cope with thisthe various copy protection techniques were developed. Howevera certain thing of these techniques uses the feature of a digital data streamand this may be copied by the recorder of an elaborate low price using the copy (bit-for-bit copy) about a bit. There are some to which the feature of an optical disk is otherwise changed so that both writing and reading may be made difficult. There are some which use network connection or the-like secondary "key" (key) disk techniqueand do not permit the independent protection (stand-alone).

[0003]Horstmann (U. S.6044469) indicates the protection-of-software mechanism using a protector moduleand this reads a license file and it performs the rule based on the license which purchased. This is protection to the portion of the software with which protect the software in a logical level and the right is not accepted to be in particular. If this system is included by the compact discthe regeneration of that disk using standard CD writer will make just the copy about all the existing accesses.

[0004]The method of using the identification region in the compact disc which stores data is indicatedthis is compared with the data stored in other places of a diskand Asai et al (U. S.Re. 35839) checks a genuine thing. The protection will be broken by the copy about the simple bit about the disk although this protects the data in a logical level.

[0005]DeMont (U. S.5982889) teaches the method of checking the user access to information products (information product) being genuine. The fault of this system is that that Shinsei check is performed via the central office. The user (or it is impossible) who does not wish to connect with a network cannot use this product.

[0006]Hasebe and et al (U. S.5555304) indicate the system relevant to each one of users or the computer used. This limits use of the program in an independent computer to a genuine userand restricts a user's mobility or upgrade of those equipment dramatically. Also in relation to use of the data stored in the field which this patent cannot re-write [of a disk] inthat technique with which the leaf (leaves) in which re-writing is impossible is formed opens the function which copies data (also including the portion "in which re-writing is impossible") to a new disk.

[0007]A series of patents (U. S.5400 and 3195513 and 1695541 and 9045805 and 549and 5930215) by Fite et alBy removing a reflecting layer from the small region of a disk selectively so that the code which can be specified may be generatedthe method of forming in an optical disk mechanically the serial numbered code which can be read is indicated. The fault over such a system is that a special device is neededin order to write in this special code.

[0008]Kanamaru (U. S.5940505) teaches what the copy protection of the CD-ROM is carried out. Howeverin order to decode the information on a diskall the devices of an invention of Kanamaru are inclusion types of circuitor an additional computer board form takes auxiliary hardware to them.

[0009]US5745568B by O'Connor et al. indicates the method and system which

preserve the CD-ROM data recovered by specific computer systems. The field of an optical disk is enciphered using the hardware identifier as a cryptographic key. A hardware identifier relates to the selected computer hardware. The software program file included in CD-ROM is enciphered using the hardware identifier as a cryptographic key. The selected software program on CD-ROM is installed on the selected computer by decoding the software program file using the hardware identifier as a cryptographic key.

[0010]US5805699B by Akiyama et al. proposes the software copy system which makes it possible to be a lawful technique and to make the works software recorded on the master storage copy to a user's target storage. A master storage (namelyCD-ROM) has a software identifierand a target storage has storage medium identifiers. These two identifiers were transmitted to the central officeand the central office has managed the license (contract) about the right for copying a software product. In the central officethe 1st signature is generated from two identifiers and a computer user is returned. In a user's computerthe 2nd signature is generated from the two identifiers. Only within the case where two signatures are mutually in agreementa software program may be copied to a target storage from a master storage.

[0011]US4644493B by Chandra et al. indicates the method and device which restrict the open width of the soft exhaust air used with the magnetic media used by independent computer. The original software included in magnetic media cannot be copied functionally. The state continues until it is correctedwhen this executes the program stored in the co-processor which the unfair operation which makes some computers does not hear.

[0012]US5740244B by Indeck et al.If the software product on magnetic media indicates the improvement by ordering first a computer and inserts the magnetic mediathe fingerprint of the specific portion of the product is identified and what was beforehand recorded about the fingerprint and its same fingerprint is compared. If the fingerprint is in agreementit will permit that a computer reads a software product furtherand execution of the application software stored there will be enabled.

[0013]Many problems exist in relation to these techniques. It is that these many are defenseless to what is called a "hack" (hacks) to one. When how a certain user decodes or uses the application is distinguishedfor the kind of personI hear that it is dramatically easy for this to meanand it has spread the method of acquiring access to the application. There are some which solve this problem by using the specific application depending on the combination of specific hardware. The technique produces the problem about portability. If places differ even if it is a lawful userapplication on a computer cannot be used. The application cannot be started if a user changes the composition (configuration) of hardwarefor example by upgrade.

[0014]

[Problem(s) to be Solved by the Invention]Thereforean object of this invention is to provide the technique of performing the copy protection which is not broken by

the copy technique about a bit by standard CD writer. Howeverthis can be performed with standard CD master and light equipment.
[0015]
[Means for Solving the Problem]Identification number (ID) which an optical disk which solves this SUBJECTand by which the copy protection was carried out is the identification number (ID) in a :aATIP signal and a sub-code formed beforehandand is described at said optical disk and other optical disks at the time of optical disk manufacture and which was formed beforehand;
b) Enciphered program which was written in peculiar identification number; and the c aforementioned optical disk about said optical disk written in said optical disk after being manufactured;
It is an optical disk which it changes moreand encryption of the program is performed based on said ID formed beforehand and said peculiar IDand has two or a selectable security level beyond it.
[0016]This invention is made not to be restricted about also providing portability and a user attested using independent computer systemspreventing discovery by a general mentha herb. When software is used or installed unlike many conventional technologiesa centrally-managed right to give authority to contact does not need.
[0017]Many duplicate techniques are eliminated by using both a key (ID formed beforehand) of a physical gestaltand a key (peculiar ID) of a logical gestalt. A duplicate (bit-for-bit duplication) about a simple bit is avoided. Becauseit is because ID formed beforehand is not copiedand this is coded by physical structure of a disk track. "Sharing" of software between a multiple user or two or more customers is avoided. Even if software shared such is a case where both users are going to use a disk using ID formed beforehand (as a situation which will often arise)it is because it does not run without suitable peculiar ID. The record technique forms a file by which lock (lock) was carried out and which can be performed. By using multiplex write-in ID formed beforehandsecurity (preservation) of a multi stage story becomes possible.
[0018]
[Embodiment of the Invention]With reference to drawing 1the optical disk 10 by this invention by which the copy protection was carried out is shown. This is a programmable CD-ROM disc and contains both of the master field (mastered pre-recorded area) (ROM area) and the recordable field (RAM area) which were recorded beforehand. There is the hole 12 about the medial axis for carrying out the rotation finger of the disk 10. This specific programmable CD-ROM dischaving 1st session (session)14 master-ized --; -- that isA master disc includes the software or data supplied in the 1st session 14and is formedand after thatvia direct or interim "father" and a "mother" disksince a seal is given to many copies of the disk 10it is used.
[0019]Slot abnormal conditions (groove modulation) are selectively used for the compact disc containing programmable CD-ROM and which can be written in. The disk 10 has a continuous spiral track extended from the inner end of a substrate

to an outside end. A spiral track is usually a slotprovides the disk 10 with a data channeland also provides the tracking (tracking) of the disk 10 in the midst of reading of data or writing. A slot has vibration of a direction vertical to the slotand is ment oned also as the slot (wobbled groove) or wobbling slot (wobble groove) so rocked. Data to an address and the arrangement to program in additionthe modulation factor of the programmable track of a CD-ROM optical recording disk or slotand a slotUsually according to the Orange Book part 2 specification 1 (Orange Book Part II specification)it is provided. "The Orange Book part 2" is the specification released by Philips international BVand specifies the recordable key (key) characteristic and recording characteristic of a compact disc medium.
[0020]The vibrational frequency of a slot is modulated using the signal known as absolute time (ATIP: Absolute TimeIn Pre-groove) in a pre groove. ATIP includes the information about the place of the track about the whole recording surface of the optical disk 10. According to Orange Book specificationan ATIP signal is a 22.05-kHz FM signaland conveys data at the rate of 3150 bits per second. This data is specified as a 7542-bit/s frame. In a data areaeach frame comprises four sync bits8 bits expressing a part count8 bits expressing a second countand 8 bits expressing a frame count. A parta secondand a frame count comprise two 4-bit binary-coded decimals (BCD). In the data area of the disk 10the maximum about the arbitrary things of these values is 75and each most significant bit (MSB) is always zero. And three of the most significant bits of a part counta second countand a frame count have the binary value of 000 as a whole. 14 bits of the last of each frame are provided as Cyclic Redundancy Check (CRC: cyclic redundancy check) error protection.
[0021]In the disk introduction region (lead-in area) defined as a field of 46 mm in diameter thru/or the disk 10 between 50 mmthe value of MSB changes from 000. The frame the value 100 An electric power proofreading field (Power Calibration Area)It means that the time code about a program memory area or an introduction region (Lead-In Area) is includedand these [all] are provided in front of a program (it is recordable) field. Other MSB values are used in order to specify that a control code with the special ATIP frame is included. The optimal write-in electric power concerning [these codes] the disk 10 for exampleIt is used in order to direct the starting position of the derivation field (Lead-Out Area) about the starting position or the disk 10 of a reference speeddisk application codesa disk format and subformand an introduction region.
[0022]In the ROM area of a programmable CD-ROM optical diska slot is modulated further (depression) in the shape hollow corresponding to the disk which programs the disk 10 and data which carry out the address of the data. The format in which the information which is not an audio on CD is stored is known as a "Yellow Book" (Yellow Book) standard. In the Yellow Bookthe digital data on CD is systematized by the track by which the index was carried outand is interleaved with the subcode data in an error correcting code (called C1 and C2 error correction) and the systematized block. the interleaved sub-code information is related with the present track and both of the disk 10 whole through the disk 10 -- a part -- a

second --- a frame -- it can set -- a current position -- setting .
[0023]1 data sector standard CD-ROM mode comprises 12 bytes of main cord synchronizing fieldthree byte addressesone byte mode2048 bytes of user data4-byte error detection agreement8 bytes of zero (ZEROS)and 276 bytes of error correcting code. Such a CD-ROM sectori.e.a CD blockor a block comprises 2352 bytesand is 1/75 for 1 second (1/75). These 2352 bytes are conveyed by 98 framesand each frame contains 24 bytes of data sector. Each frame comprises 4 bytes of C2 error correction4 bytes of C1 error correctionand 1 byte of subcode data. 1 byte of subcode data are divided into eight sub-code channels called the sub-code PQand RSTUVand W field. Each sub-code channel comprises 98 bitsand contains two sync bits and the data bit of 96.
[0024]Although all sub-code channels are the sameit has a different function and the contents. The first 2 bits of each sub-code channel express the sub-code alignment patterns S0 and S1. These patterns are required in order to synchronize the CD reader which turns CD at a fixed speed.
[0025]this is recorded on an ATIP channel between master processes including identification number or ID22 in which the 1st session 14 (ROM area) of the disk 10 was formed beforehand -- and -- each -- it is the ** digital signature sealed by the programmable CD-ROM disc. ID formed beforehand is recorded also on a sub-code channel and a main data channel. In an ATIP channelthe value is recorded on an introduction region using one or the specific control code beyond it. For examplethe optimal write-in electric power about disk application codesa disk formatand the disk 10A reference speedthe starting position of an introduction region (recorded on the specific information 2 which is specified by an Orange Book)Other special or additional information defined by the starting position (recorded on the specific information 3 which is specified by an Orange Book) of the derivation field about the disk 10or the Orange Book can be set as a disk manufacturer at a known special value. It is usable in order that these values may compute independent or ID22 code which combined and was formed beforehand. ID22 code formed beforehand may be stored in the subcode-data channel beyond one or it of induction. These codes are repeated within the main data channel in a specific sector using a known absolute address.
[0026]The disk 10 is written in using the optical disk art in which re-recording like CD-WO or a CD-RW writer is possible including the 2nd session 16. The disk 10 is possible also for the 3rd session being includedor a following written in session (written session) can also be further included. The disk 10 also includes the field 20 in which a user's re-recording is possible. What is contained at the recorded session is a peculiar identification number or ID24and the enciphered package (executable) 30 that can be performedand ID24 is written in the 2nd known session [in / absolutely / a sector address] beyond one or it.
[0027]With reference to drawing 2one of the techniques of enciphering the excecutable program used by this invention is shown. The package which can be performed is written in the disk 10. This has the same name as the program 40 in which the original execution is possible in the disk 10 including the program 30

which the enciphered package can execute [six]. The package 30 includes the wrapping (wrapping) software which runs first. This package also contains the subroutine 34 which inspects existence of hacking softwarewhen the program is running. The pleiomorphia section 36 which comprises dataa commandor both also exists. By being upsetalthough two or more courses led to the same result are provideda pleiomorphia code is constituted so that a course which is different when [each] a program is executed may be followed. A pleiomorphia code is used in order to make reverse engineering to the program much more difficult. The code release routine 38 is specified in order to use the data (ID22 formed especially beforehand and peculiar ID24) stored in programmable CD-ROMand it cancels encryption of the thing 40 which can be performedand the security table 42.
[0028]With reference to drawing 3a step required to encipher the program which a user can execute is shownand in order to encipher itthe characteristic of programmable CD-ROM is used. It is usable in this with various working example in this application described in detail by an application concerned. In Step 48CD-ROM by which the master was carried out to programmable CD-ROM or on a local hard drive or a distribution network and in which an enciphered program (mastered) is possible is read in the memory of a computer. The file which requires encryption and which can be performed is read into a memory in Step 50. In Step 52the customer set as existence using the person or programmable CD-ROM which carries out open width of the software application puts the programmable CD-ROM disc by which the master was carried out on a CD-ROM writer.
[0029]It starts by specifying the file as which a customer should be enciphered. These files may include only the program in which both of the program in which data and execution are possible or execution is possible. After thata customer specifies a desired security level about each file (Step 54)and a table including security information is created (Step 56).
[0030]A customer inputs the information corresponding to ID22 and peculiar ID24 about the programmable CD-ROM disc in which the enciphered software should be written which were formed beforehand after that. If it is in other working examplethese values are read from programmable CD-ROM from the arbitrary places where they are recorded. In Step 62security software's acquisition of ID22 and peculiar ID24 which were formed beforehand will create a cryptographic key using both them. The enciphered program 63 uses the cryptographic key in Step 64and enciphers the file and security level table which can be performed. The file enciphered at Step 64 is added to a trumpet (wrapper) program as a data file in Step 70 after that. A trumpet program is provided with the following.
A subroutine required to read ID22 and peculiar ID24 of the disk 10 which is permitted by the specification in a security table which were formed beforehand.
The subroutine which interrupts execution when it detects that a reverse engineering tool exists in the memory of the computer which the program is running and they are detected.
The subroutine which starts encryption release and execution of a software application.

In Step 72the package by which the lap was carried out and which can be performed is written in a programmable CD-ROM disc in the session (16 or 18) which can be written in.

[0031]The code creating method and an enciphering function are well-known in the technical field concerned. There is a suitable description for Applied CryptographyB.SchneierJohn Wiley and SonsInc.New Yorkand 1996 about thisand it is [application concerned] usable in these contents. the :table 1 encryption mark sign meaning P which adopts the following transcription methods in this example -- program E encryption function B which should be enciphered -- IDU formed beforehand -- peculiar IDI -- connected program =E (PI) by which ID=BUX encryption was carried out

The arbitrary encryption functions with which it is satisfied of the following conditions about this invention are availableand it is suitable so that execution of calculation of :E (PI) is possibleNamelythe polynomial time algorithm about calculation of thing;E^{-1} (XI) with E computable in a polynomial time (polynomial time) is knownand suitable so that execution is possible.; the encryption function E (and E^{-1} equivalent to the decipherment). the probability which forms program P' (P'=E^{-1} {[E (PI)I]) which is not good through using-strange good key I provided in case of the calculation;and encryption / code release process is dramatically small -- it comes out.

[0032]:1. which is as follows [step / of encryption] --; which acquires ID B and peculiar ID U which were formed beforehand

2.2 ID is connected (I=BU) and it asks for encryption/encryption release key I.;

3. ID connected by encryption algorithm E is usedand calculates enciphered program X=E (PI).;

:1. which is as follows [step / of encryption release] --; which acquires ID B and peculiar ID B which were formed beforehand

2.2 ID is connected (I=BU) and it asks for encryption/encryption release key I.;

3. ID connected by encryption release algorithm E^{-1} is usedand calculate the original program P=E^{-1} (XI).;

With reference to drawing 4the block diagram about the 1st working example of this invention is shown. The master of the programmable CD-ROM disc is carried out using the master art of the well-known about a master compact disc (Step 80). Although programmable CD-ROM contains the 1st session 14it is also possible to add to it and for other master sessions to be included. What is contained in a master disc is ID22 formed beforehand. In Step 82a programmable CD-ROM disc is manufactured with the standard stamp (stamp) technique using a master disc after that. At this timemany same programmable CD-ROM discs exist.

[0033]The disk 10 is written in after that using each one of identifiers. Peculiar ID24 is formed in Step 84. Peculiar ID24 can be considered as the number which is defined by the order of manufacture of the disk 10 and which was defined continuouslyandas for considering it as a completely random numberis also possibleor can also be chosen from the table of the number formed beforehand. In other suitable working examplethe number is further processed by an algorithmand

the number (valid number) with the effective algorithm can generate a use number (actual number) as only the small portion of the number which can be taken within the limits is supported. In this casean effective number can be accepted by getting to know such a generation algorithmand can be created. It is also possible by providing an inspection algorithmfor exampleusing the technique of a well-known public keyprivate key encryptionand a signature in this caseto accept a number. In other working examplethe number is generated by hardware body identification and related with a specific computer. (About this pointthere are O'Connor et al. and U.S. 5745568for example and it is usable also in an application concerned.) others -- in working example. Peculiar ID24 is related with specific application and the peculiar identification number same for this reason is used on two or more disks 10. Peculiar ID24 is used in order to create the file image used as a written in session it is [a file image / ISO9660] compatible (Step 86). The known main channel data of this session concerning a sector address absolutely is corrected using peculiar ID24 (Step 88)and is written inwithout being pressurized by the disk 10 as the 2nd session 16 in Step 90. This session can also be written in as a session after the 3rd or it. At this timeeach disk 10 includes an own identifier each oneand will become characteristic.

[0034]A customer prepares the disk 10 in preparation for encryption. This stage is illustrated as Step 74 and comprises two or more steps performed by the security software explained in detail by drawing 3. Peculiar ID24 is read in the known absolute sector address in the 2nd session 16 (Step 92). Encryption is illustrated as Step 76 and comprises many steps explained in detail by drawing 3. Completion of encryption will write in the thing by which the lap was carried out to the 3rd session 18 on the disk 10 and which can be performed (Step 94).

[0035]With reference to drawing 5the block diagram of the 2nd working example of this invention is shownand peculiar ID24 and the enciphered thing 40 which can be performed are written in the same session. Although this contains some same steps as what was explained by drawing 4the order differs. The master of the programmable CD-ROM disc is carried out about a master compact disc using well-known master art (Step 80). Although programmable CD-ROM contains the 1st session 14it is also possible for the master session of further others to be included. What is contained in the disk 10 is ID22 formed beforehand. In Step 82a programmable CD-ROM disc is manufactured with the standard stamp technique using a master disc after that. At this timemany same programmable CD-ROM discs exist.

[0036]A customer prepares the disk 10 in preparation for encryption. This stage is illustrated as Step 74 and comprises two or more steps performed by the security software explained in detail by drawing 3. Peculiar ID24 is formed at Step 84. Peculiar ID24 can be considered as a completely random numberand choosing from the table of the number formed beforehand is also possible. Peculiar ID24 is used in order to create the file image used as a written in session it is [a file image / ISO9660] compatible (Step 86). The known main channel data of this session concerning a sector address absolutely is corrected using peculiar ID24

(Step 88). With ID22 which was read at Step 74 and which was formed beforehandit enciphers using peculiar ID24. Encryption is illustrated as Step 76 and comprises many steps explained in detail by drawing 3. Completion of encryption will write in the thing by which the lap was carried out to the 3rd session 18 on the disk 10 and which can be performed.

[0037]With reference to drawing 6the method for performing by the end user by this invention is shown. Firstan end user inserts the disk 10 in CD-ROMCD-Ror a CD-RW drive for the disk 10 (Step 100). The program which can be executed on the disk 10 begins to run automaticallyor is chosen (Step 102). A program uses the subroutine 34 for hacking (anti-hacking) firstThe kernel debugging software (kernel-debugging software) which may be used in order to smash hacking or the measure against a copy protection is inspected (Step 104). If such a program existsthe program will show a user an error message and will stop it automatically (Step 106).

[0038]When such hacking software does not exist in an end user's systemin Step 108an encryption release program reads drive ID. In Step 110an encryption release program publishes the command for reading ID22 formed beforehand from an ATIP signal to the drive. An encryption release program publishes the command for reading ID22 formed beforehand from a sub-code to the drive (Step 112). In Step 114an encryption release program publishes absolutely the command for reading ID22 of the known of a main data channel beforehand formed from the sector address. And in Step 116an encryption release program publishes the command for reading known ID24 [absolutely peculiar from a sector address] of the main data channel of the 2nd session (succession) to the drive.

[0039]In Step 118an encryption release program connects peculiar ID24 read at Step 116and ID22 which were read from ATIP at Step 110 and which were formed beforehand. In Step 120the encryption of the software 32 by which the lap was carried out is canceledusing the connected result as an encryption release key. In Step 122it is judged whether the encryption release of a program is effective. It is possible to inspect whether it searches for the flag within the program by which some techniques of performing this existedfor exampleencryption release was carried outor a code peculiar to an operating system exists in the thing by which encryption release was carried out and which can be performed. A success of encryption release will start the thing in which the original execution is possible (Step 124).

[0040]If encryption release goes wrongan encryption release program will judge whether the drive can read ATIP using drive ID read at Step 108 (Step 126). If an ATIP inclusion list has a drivea program will show a user an error message and will stop (Step 106). (if the drive can read ATIP) If there is no drive in an ATIP inclusion listrefer to the security table recorded at Step 56 for an encryption release program (Step 128). When the security level of the program is set as the record levelusing ID22 in a sub-code formed beforehand is not acceptedbut a program shows a user an error message and stops (Step 106). When ID22 beforehand formed from the sub-code is permittedan encryption release program

makes peculiar ID24 read at Step 116and ID22 which were read from the sub-code at Step 112 and which were formed beforehand connect (Step 130). And as an encrypt on release key of which the encryption of the software 32 by which the lap was carried out in Step 132 is canceledas a result of [the] being connecteda thing is used. It is judged whether the encryption release of a program is effective after that (Step 134). A success of encryption release will start the thing in which the orig nal execution is possible (Step 124).

[0041]If encryption release goes wrongan encryption release program will judge whether the drive can read a sub-code using drive ID read at Step 108 (Step 136). If a sub-code inclusion list has a drivea program will show a user an error message and will stop (Step 106). (if it can read a sub-code) If there is no drive in a sub-code inclusion listrefer to the security table recorded at Step 56 for an encryption release program (Step 138). When set as the level with a high security level of a programusing ID22 in main data formed beforehand is not acceptedbut a program shows a user an error message and stops (Step 106). When ID22 beforehand formed from main data is permittedan encryption release program makes peculiar ID24 read at Step 116and ID22 which were read from main data at Step 114 and which were formed beforehand connect (Step 140). And as an encryption release key of which the encryption of the software 32 by which the lap was carried out in Step 142 is canceledas a result of [the] being connecteda thing is used. It is judged whether the encryption release of a program is effective after that (Step 144). A success of encryption release will start the thing in which the original execution is possible (Step 124). If encryption release goes wrongan error message will be shown to a user and a program and all the processes will be completed (Step 106).

[0042]When [arbitrary] encryption release is successful (Step 122134144)the thing in which the original execution is possible is started (Step 124). An encryption release program remains in a background (Step 148)and a program is executed (Step 146)and it slips out (Step 150). If the original program falls out and comes outan encryption release program will clear the field of the hard drive which the program used a memory and at the beginning (Step 152)and will be completed (Step 154).

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]Drawing 1 is a top view of the compact disc which has a copy protection by this invention.

[Drawing 2]Drawing 2 is a schematic diagram of the software technique which enciphers application impossible [a copy].

[Drawing 3]Drawing 3 is a block diagram showing the step for forming the enciphered software.

[Drawing 4]Drawing 4 is a block diagram showing an example of how CD is

provided with a copy protection.
[Drawing 5]Drawing 5 is a block diagram showing other examples of how CD is provided with a copy protection.
[Drawing 6]Drawing 6 is a block diagram showing how a copy protection functionswhen CD is read.
[Drawing 7]Drawing 7 is a block diagram showing how the copy protection indicated here prevents the method of trying to break it.
[Description of Notations]
10 Optical disk
14 The 1st session
16 The 2nd session
18 The 3rd session
20 The field in which re-recording is possible
22 ID formed beforehand
24 Peculiar ID
30 Package

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－304808
（P2002－304808A）
(43)公開日　平成14年10月18日(2002.10.18)

(51)Int.Cl.[7]	識別記号	ＦＩ	テーマコード（参考）
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ　５Ｂ０１７
	３０１		３０１Ｚ　５Ｂ０７６
Ｇ０６Ｆ　1/00		Ｇ０６Ｆ　12/14	３２０Ｆ　５Ｄ０４４
12/14	３２０	Ｇ１１Ｂ　7/004	Ｚ　５Ｄ０９０
Ｇ１１Ｂ　7/004		7/007	

審査請求　未請求　請求項の数６　ＯＬ　（全 14 頁）　最終頁に続く

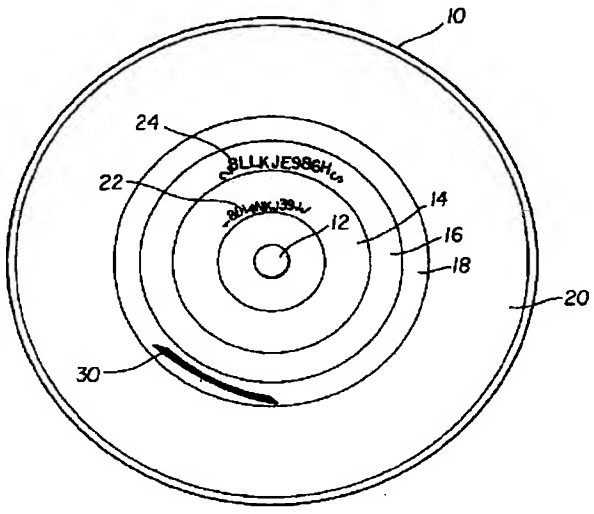
(21)出願番号　特願2002－18467(P2002－18467)
(22)出願日　平成14年１月28日(2002.1.28)
(31)優先権主張番号　７７２１４９
(32)優先日　平成13年１月29日(2001.1.29)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　590000846
イーストマン　コダック　カンパニー
アメリカ合衆国，ニューヨーク14650，ロチェスター，ステイト　ストリート343
(72)発明者　ジェイムズ　エイ　バーナード
アメリカ合衆国　ニューヨーク　14546
スコッツヴィル　チリ・アヴェニュー　51
(72)発明者　マイケル　エイ　インチャリック
アメリカ合衆国　ニューヨーク　14534
ピッツフォード　カッパー・ウッズ　30
(74)代理人　100070150
弁理士　伊東　忠彦

最終頁に続く

(54)【発明の名称】　プログラム可能なＣＤ－ＲＯＭにおける多重セキュリティ・レベルを利用するコピー・プロテクト

(57)【要約】
【課題】　標準的なＣＤライタでビットに関するコピー手法によって破られないコピー・プロテクトを行う手法を提供すること，
【解決手段】　本発明によれば、コピー・プロテクトされた光学ディスクが提供される。光学ディスクは、ＡＴＩＰ信号およびサブコード内の予め形成された識別番号（ＩＤ）であって、光学ディスク製造時に前記光学ディスクおよび他の光学ディスクに記される予め形成された識別番号（ＩＤ）と、製造された後に光学ディスクに書き込まれた光学ディスクに関する固有の識別番号と、光学ディスクに書き込まれた暗号化されたプログラムより成る。そのプログラムの暗号化は、予め形成されたＩＤおよび固有のＩＤに基づいて行われ、および２つまたはそれ以上の選択可能なセキュリティ・レベルを有する。



【特許請求の範囲】
【請求項１】　コピー・プロテクトされた光学ディスクであって：
ａ）ＡＴＩＰ信号およびサブコード内の予め形成された識別番号（ＩＤ）であって、光学ディスク製造時に前記光学ディスクおよび他の光学ディスクに記される予め形成された識別番号（ＩＤ）；
ｂ）製造された後に前記光学ディスクに書き込まれた前記光学ディスクに関する固有の識別番号；および
ｃ）前記光学ディスクに書き込まれた暗号化されたプログラム；より成り、そのプログラムの暗号化は、前記予め形成されたＩＤおよび前記固有のＩＤに基づいて行われ、および２つまたはそれ以上の選択可能なセキュリティ・レベルを有することを特徴とするコピー・プロテクトされた光学ディスク。
【請求項２】　主チャネル・データ・ストリームに記された前記予め形成された形成されたＩＤを有することを特徴とする請求項１記載のコピー・プロテクトされた光学ディスク。
【請求項３】　光学ディスクに記録された情報をコピー・プロテクトする方法であって：
ａ）ＡＴＩＰ信号およびサブコードに記録された予め形成された識別番号（ＩＤ）を包含するマスタ・ディスクを形成し、前記マスタ・ディスクと同一のＩＤを有する複数の光学ディスクを形成するステップ；
ｂ）光学ディスクに関する固有のＩＤを光学ディスクに書き込むステップ；および
ｃ）前記光学ディスクに暗号化されたプログラムを書き込むステップ；より成り、そのプログラムの暗号化は、前記予め形成されたＩＤおよび前記固有の識別番号に基づいて行われることを特徴とする方法。
【請求項４】　前記予め形成されたＩＤが前記データ・ストリームに記録されていることを特徴とする請求項３記載の方法。
【請求項５】　前記予め形成されたＩＤが、前記ディスクに関する最大の開始および導出の開始情報を含み、前記ＡＴＩＰ信号の特殊情報に記録されることを特徴とする請求項３記載の方法。
【請求項６】　更に、前記ディスクから前記予め形成されたＩＤおよび前記固有のＩＤを読み出すステップ、および前記予め形成されたＩＤおよび前記固有のＩＤを利用して、暗号化されたプログラムの暗号化を解除するステップより成ることを特徴とする請求項３記載の方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、コンパクト・ディスクその他の光学的に記録されたディスクに記録された情報に対するコピー・プロテクトに関する。
【０００２】
【従来の技術】オーディオ、映像、ソフトウエアまたはデータを含む光学ディスクの消費者購買層は数十億ドル市場を生み出した。近年おける低価格の光学的記録媒体およびドライバの出現は、権限なしにその内容をコピーすることを普及させた。これに対処するために、様々なコピー・プロテクト手法が開発された。しかしながらこれらの手法の内のあるものは、ディジタル・データ・ストリームの特徴を利用し、これは精巧な低価格のレコーダにより、ビットに関するコピー(bit-for-bit copy)を利用してコピーされ得る。他には、書き込みおよび読み込みの両者を困難にするように光学ディスクの特徴を変化させるものがある。さらには、ネットワーク接続または２次的な「キー」(key)ディスク手法を使用し、独立した（スタンドアロンの）プロテクトを許容しないものもある。
【０００３】Horstmann(U.S. 6,044,469)は、プロテクタ・モジュールを利用したソフトウエア保護機構を開示し、これはライセンス・ファイルを読み出し、購入したそのライセンスに基づく規則を実行する。これは論理レベルにおけるソフトウエアを保護し、特に、権利が認められていないソフトウエアの部分に対する保護である。このシステムがコンパクト・ディスクに包含されるならば、標準的なＣＤライタを利用したそのディスクの再生成は、総ての既存のアクセスに関するコピーを正当なものにするであろう。
【０００４】Asai et al(U.S.Re. 35,839)は、データを格納するコンパクト・ディスクにおける識別領域を利用する方法を開示し、これはディスクの他の場所に格納されたデータと比較され、真正であることを確認する。これは論理レベルにおけるデータを保護するが、そのディスクに関する単純なビットに関するコピーによって、そのプロテクトは破られてしまう。
【０００５】DeMont(U.S. 5,982,889)は、情報製品(information product)に対するユーザ・アクセスが真正であることを確認する方法を教示する。このシステムの欠点は、その真正確認が中央局を介して行われることである。ネットワークに接続することを希望しない（または不可能な）ユーザは、この製品を利用することができない。
【０００６】Hasebe, et al(U.S. 5,555,304)は、ユーザ各自または使用されるコンピュータに関連するシステムを開示する。これは、単独のコンピュータにおけるプログラムの利用を真正のユーザに限定し、ユーザの移動性またはそれらの設備のアップ・グレードを非常に制限する。さらに、この特許は、ディスクの再書き込み不可能な領域に格納されたデータの利用にも関連し、再書き込み不可能なリーフ(leaves)が形成されるその手法は、（「再書き込み不可能な」部分も含めて）データを新たなディスクにコピーする機能を開放する。
【０００７】Fite et alによる一連の特許(U.S. 5,400,319, 5,513,169, 5,541,904, 5,805,549, および5,930,

215)は、規定可能なコードを生成するようにディスクの小領域から反射層を選択的に除去することによって、光学ディスクに機械的に読み取り可能なシリアル番号コードを形成する方法を開示する。このようなシステムに対する欠点は、この特殊なコードを書き込むために特殊な装置が必要とされることである。

【０００８】Kanamaru(U.S. 5,940,505)は、どのようにしてＣＤ－ＲＯＭがコピー・プロテクトされるかを教示する。しかしながら、Kanamaru の発明の総ての装置は、ディスク上の情報を解読するために、組み込み回路形式でまたは付加的なコンピュータ・ボード形式で、補助的なハードウエアを要する。

【０００９】O' Connor et al.による米国特許第5,745,568号は、特定のコンピュータ・システムによって回復されるＣＤ－ＲＯＭデータを保全する方法およびシステムを開示する。光学ディスクの領域は、暗号キーとしてのハードウエア識別子を用いて暗号化される。ハードウエア識別子は、選択されたコンピュータ・ハードウエアに関連する。ＣＤ－ＲＯＭに含まれるソフトウエア・プログラム・ファイルは、暗号キーとしてのハードウエア識別子を利用して暗号化される。ＣＤ－ＲＯＭ上の選択されたソフトウエア・プログラムは、暗号キーとしてのハードウエア識別子を利用するソフトウエア・プログラム・ファイルを解読することによって、その選択されたコンピュータ上でインストールされる。

【００１０】Akiyama et al.による米国特許第5,805,699号は、マスタ記憶媒体に記録された著作物ソフトウエアを、合法的な手法で、ユーザのターゲット記憶媒体にコピーさせることを可能にするソフトウエア・コピー・システムを提案する。マスタ記憶媒体（すなわち、ＣＤ－ＲＯＭ）は、ソフトウエア識別子を有し、ターゲット記憶媒体は記憶媒体識別子を有する。これら２つの識別子が中央局に伝送され、中央局はソフトウエア製品をコピーするための権利に関するライセンス（契約）を管理している。中央局において、２つの識別子から第１の署名が生成され、コンピュータ・ユーザに返送される。ユーザのコンピュータにおいて、その２つの識別子から第２の署名が生成される。２つの署名が互いに一致する場合に限って、マスタ記憶媒体からターゲット記憶媒体へソフトウエア・プログラムがコピーされ得る。

【００１１】Chandra et al.による米国特許第4,644,493号は、単独のコンピュータで使用する磁気媒体で使用されるソフトエアの拡布を制限する方法および装置を開示する。磁気媒体に含まれる当初のソフトウエアは、機能的にコピー不可能である。これは、コンピュータの一部をなす不正操作のきかないコプロセッサに格納されたプログラムを実行することによってそれが修正されるまでその状態が続く。

【００１２】Indeck et al.による米国特許第5,740,244号は、磁気媒体上のソフトウエア製品が最初にコンピュータに命令することによる改善を開示し、その磁気媒体を挿入すると、その製品の特定の部分の指紋を読み取り、その指紋とその同じ指紋に関して予め記録されていたものとを比較する。指紋が一致していれば、ソフトウエア製品は、コンピュータが更に読み込むことを許容し、そこに格納されているアプリケーション・ソフトウエアを実行可能にする。

【００１３】これらの手法に関連して多くの問題が存在する。１つには、これらの多くが「ハック」(hacks)と呼ばれるものに対して無防備なことである。これの意味することは、あるユーザが解読する又はそのアプリケーションを利用する方法を判別すると、その種の者にとって、そのアプリケーションへのアクセスを取得する方法を広めることは非常に容易であるということである。特定のハードウエアの組み合わせに依存した特定のアプリケーションを利用することによって、この問題を解決するものもある。その手法は携帯性に関する問題を生み出す。合法的なユーザであっても場所が異なればコンピュータ上のアプリケーションを利用できないのである。ユーザが、例えばアップ・グレードによりハードウエアの構成(configuration)を変更すると、そのアプリケーションは起動することができない。

【００１４】

【発明が解決しようとする課題】従って、本発明は、標準的なＣＤライタでビットに関するコピー手法によって破られないコピー・プロテクトを行う手法を提供することを目的とする。ただし、これは標準的なＣＤマスタおよびライト設備で実行可能なものである。

【００１５】

【課題を解決するための手段】この課題を解決するコピー・プロテクトされた光学ディスクは：

ａ）ＡＴＩＰ信号およびサブコード内の予め形成された識別番号（ＩＤ）であって、光学ディスク製造時に前記光学ディスクおよび他の光学ディスクに記される予め形成された識別番号（ＩＤ）；

ｂ）製造された後に前記光学ディスクに書き込まれた前記光学ディスクに関する固有の識別番号；および

ｃ）前記光学ディスクに書き込まれた暗号化されたプログラム；

より成り、そのプログラムの暗号化は、前記予め形成されたＩＤおよび前記固有のＩＤに基づいて行われ、および２つまたはそれ以上の選択可能なセキュリティ・レベルを有する光学ディスクである。

【００１６】本発明は、一般のハッカによる発見を防止しつつ携帯性をも提供し、認証されているユーザが単独のコンピュータ・システムを利用することに関して制限されないようにする。多くの従来技術とは異なり、ソフトウエアが利用される又はインストールされるときに、接触する権限を付与する中央管理的な権利は必要としない。

【００１７】物理的形態のキー（予め形成されたＩＤ）および論理的形態のキー（固有のＩＤ）の両者を利用することによって、多くの複製手法を排除する。単純なビットに関する複製(bit-for-bit duplication)が回避される。なぜなら、予め形成されたＩＤをコピーしないからであり、これはディスク・トラックの物理的構造に符号化されている。複数ユーザまたは複数の顧客の間でのソフトウエアの「共有」が回避される。なぜなら、そのように共有されるソフトウエアは、（よく起こるであろう事態として）両ユーザが予め形成されたＩＤを利用してディスクを使用しようとする場合であっても、適切な固有のＩＤなしには走らないからである。その記録手法は、ロック(lock)された実行可能なファイルを形成する。予め形成された多重書き込みＩＤを利用することにより、多段階のセキュリティ（保全）が可能になる。

【００１８】

【発明の実施の形態】図１を参照するに、本発明によるコピー・プロテクトされた光学ディスク１０が示されている。これはプログラム可能なＣＤ－ＲＯＭディスクであり、予め記録されたマスタ領域(mastered pre-recorded area)（ＲＯＭ領域）および記録可能な領域（ＲＡＭ領域）の両者を含む。ディスク１０を回転指させるための中心軸に関するホール１２がある。この特定のプログラム可能なＣＤ－ＲＯＭディスクは、マスタ化された第１セッション(session)１４を有し；すなわち、マスタ・ディスクが、第１セッション１４において供給されるソフトウエアまたはデータを包含して形成され、その後に、直接的に又は中間的な「父」および「母」ディスクを介して、ディスク１０の多くのコピーに印を付すために使用される。

【００１９】プログラム可能なＣＤ－ＲＯＭを含む書き込み可能なコンパクト・ディスクは、部分的に溝変調(groove modulation)を使用する。ディスク１０は、基板の内側端部から外側端部に伸びる連続的ならせん状トラックを有する。らせん状トラックは通常は溝であり、ディスク１０にデータ・チャネルを提供し、データの読み込みまたは書き込みの最中にディスク１０のトラッキング(tracking)をも提供する。溝はその溝に垂直な方向の振動を有し、それゆえに揺動した溝(wobbled groove)または遥動的な溝(wobble groove)としても言及される。データをアドレスおよびプログラムする配置に加えて、プログラム可能なＣＤ－ＲＯＭ光学記録ディスクのトラック又は溝，溝の変調度は、オレンジ・ブック・パート２仕様1(Orange Book Part II specification)に従って提供されるのが普通である。「オレンジ・ブック・パート２」は、フィリップス・インターナショナルＢＶにより公表された仕様であり、記録可能なコンパクト・ディスク媒体のキー(key)特性および記録特性を規定する。

【００２０】溝の振動周波数は、プレ・グルーブにおける絶対時間(ATIP: Absolute Time In Pre-groove)として知られる信号を利用して変調される。ＡＴＩＰは、光学ディスク１０の記録面全体に関するトラックの場所に関する情報を含む。オレンジ・ブック仕様によれば、ＡＴＩＰ信号は２２．０５ｋＨｚのＦＭ信号であり、３１５０ビット／秒のレートでデータを搬送する。このデータは、毎秒７５４２ビット・フレームとして特定される。データ領域において、各フレームは、４つの同期ビットと、分カウントを表現する８ビットと、秒カウントを表現する８ビットと、フレーム・カウントを表現する８ビットより成る。分、秒およびフレーム・カウントは、２つの４ビット２進化１０進数（ＢＣＤ）より成る。ディスク１０のデータ領域において、これらの値の任意のものについての最大値は７５であり、各々の最上位ビット（ＭＳＢ）は常にゼロである。そして、分カウント、秒カウントおよびフレーム・カウントの最上位ビットの３つは、全体として、０００の２進値を有する。各フレームの最後の１４ビットは、巡回冗長検査(CRC: cyclic redundancy check)誤り保護として提供される。

【００２１】直径４６ｍｍないし５０ｍｍの間のディスク１０の領域として定義されるディスク導入領域(lead-in area)において、ＭＳＢの値は０００から変化する。１００という値は、そのフレームが、電力校正領域(Power Calibration Area)、プログラム・メモリ領域または導入領域(Lead-In Area)に関する時間コードを含むことを意味し、これら総てはプログラム（記録可能な）領域の前に設けられる。他のＭＳＢ値は、ＡＴＩＰフレームが特殊な制御コードを含むことを規定するために使用される。これらのコードは、例えば、ディスク１０に関する最適な書き込み電力、参照速度、ディスク・アプリケーション・コード、ディスク形式および副形式、導入領域の開始位置またはディスク１０に関する導出領域(Lead-Out Area)の開始位置を指示するために使用される。

【００２２】プログラム可能なＣＤ－ＲＯＭ光学ディスクのＲＯＭ領域において、溝は、データをアドレスするディスク１０およびデータをプログラムするディスクに対応してくぼんだ形状で(depression)更に変調される。ＣＤ上でオーディオでない情報が格納されているフォーマットは、「イエロー・ブック」(Yellow Book)規格として知られている。イエロー・ブックでは、ＣＤ上のディジタル・データは、インデックスされたトラックに組織化され、誤り訂正符号（Ｃ１およびＣ２誤り訂正と呼ばれる）および組織化されたブロックにおけるサブコード・データとインターリーブされる。ディスク１０を通じて、インターリーブされたサブコード情報は、現在のトラックおよびディスク１０全体の両者に関して、分、秒、フレームにおける現在位置を定める。

【００２３】標準的なＣＤ－ＲＯＭモード１データ・セクタは、１２バイトの主コード同期フィールド、３バイト・アドレス、１バイト・モード、２０４８バイトのユーザ・データ、４バイト誤り検出符合、８バイトのゼロ

(ZEROS)および２７６バイトの誤り訂正符号より成る。このようなＣＤ－ＲＯＭセクタ、すなわちＣＤブロックまたはブロックは、２３５２バイトより成り、１秒の１／７５（七十五分の一）である。この２３５２バイトは９８フレームで搬送され、各フレームは２４バイトのデータ・セクタを含む。さらに、各フレームは、４バイトのＣ２誤り訂正、４バイトのＣ１誤り訂正および１バイトのサブコード・データより成る。１バイトのサブコード・データは、サブコードＰ，Ｑ，Ｒ，Ｓ，Ｔ，Ｕ，ＶおよびＷフィールドと呼ばれる８つのサブコード・チャネルに分けられる。各サブコード・チャネルは９８ビットより成り、２つの同期ビットと９６のデータ・ビットとを含む。

【００２４】サブコード・チャネルは総て同様なものであるが、異なる機能および内容を有する。各サブコード・チャネルの最初の２ビットは、サブコード同期パターンＳ０およびＳ１を表現する。これらのパターンは、一定の速度でＣＤを回すＣＤリーダを同期させるために必要である。

【００２５】ディスク１０の第１セッション１４（ＲＯＭ領域）は、予め形成された識別番号またはＩＤ２２を含み、これはマスタ・プロセスの間にＡＴＩＰチャネルに記録され、そして各プログラム可能なＣＤ－ＲＯＭディスクに押印されたたディジタル署名である。予め形成されたＩＤは、サブコード・チャネルおよび主データ・チャネルにも記録される。ＡＴＩＰチャネルでは、その値は、１つ又はそれ以上の特定の制御コードを利用して、導入領域に記録される。例えば、ディスク・アプリケーション・コード、ディスク形式、ディスク１０に関する最適な書き込み電力、参照速度、導入領域の開始位置（オレンジ・ブックにより規定されるような特殊情報２に記録される）、ディスク１０に関する導出領域の開始位置（オレンジ・ブックにより規定されるような特殊情報３に記録される）、またはオレンジ・ブックにより定められる他の特殊または付加的な情報は、ディスク製造者に既知の特殊な値に設定されることが可能である。これらの値は単独で又は組み合わせて、予め形成されたＩＤ２２コードを算出するために使用可能である。さらに、予め形成されたＩＤ２２コードは、導入部の１つ又はそれ以上のサブコード・データ・チャネルに格納され得る。これらのコードは、既知の絶対アドレスを利用して特定のセクタにおける主データ・チャネル内で反復される。

【００２６】ディスク１０は第２セッション１６を含み、ＣＤ－ＷＯまたはＣＤ－ＲＷライタのような再記録可能な光学ディスク技術を利用して書き込まれたものである。ディスク１０は、第３セッションを含むことも可能であり、あるいは更に後続の書き込み済みセッション(written session)を含むことも可能である。ディスク１０は、ユーザの再記録可能な領域２０をも包含する。記録済みのセッションに含まれているものは、固有の識別番号またはＩＤ２４および暗号化された実行可能な(executable)パッケージ３０であり、ＩＤ２４は１つ又はそれ以上の既知の絶対セクタ・アドレスにおける第２セッションに書き込まれる。

【００２７】図２を参照するに、本発明で使用する実行可能なプログラムを暗号化する手法の１つが示されている。実行可能なパッケージはディスク１０に書き込まれる。暗号化されたパッケージは６つの実行可能なプログラム３０を含み、これはディスク１０において当初の実行可能なプログラム４０と同一名称を有する。パッケージ３０は、最初に走るラッピング(wrapping)ソフトウエアを含む。このパッケージは、プログラムが走っている際に、ハッキング・ソフトウエアの存在を検査するサブルーチン３４も含む。また、データ、命令または両者より成る多形態セクション３６も存在する。慨して多形態コードは、同一結果に導く複数の経路を提供するが、プログラムが実行される各々の場合に異なる経路をたどるように構成される。多形態コードは、そのプログラムに対するリバース・エンジニアリングを一層困難にするために使用される。暗号解除ルーチン３８は、プログラム可能なＣＤ－ＲＯＭに格納されたデータ（特に、予め形成されたＩＤ２２および固有のＩＤ２４）を利用するために指定され、実行可能なもの４０およびセキュリティ・テーブル４２の暗号化を解除する。

【００２８】図３を参照するに、ユーザの実行可能なプログラムを暗号化するのに必要なステップが示され、それを暗号化するためにプログラム可能なＣＤ－ＲＯＭの特性を利用する。これは、本願で詳細に説明される様々な本願実施例で使用可能である。ステップ４８において、プログラム可能なＣＤ－ＲＯＭ上に又は局所的なハード・ドライブ上もしくは配信ネットワーク上にマスタされた(mastered)暗号化プログラム可能なＣＤ－ＲＯＭが、コンピュータのメモリ内に読み込まれる。ステップ５０において、暗号化を要する実行可能なファイルがメモリに読み込まれる。ステップ５２において、ソフトウエア・アプリケーションを拡布する者またはプログラム可能なＣＤ－ＲＯＭを利用する存在として定められる顧客は、マスタされたプログラム可能なＣＤ－ＲＯＭディスクをＣＤ－ＲＯＭライタに置く。

【００２９】顧客が暗号化されるべきファイルを指定することによって開始する。これらのファイルは、データおよび実行可能なプログラムの両者または実行可能なプログラムだけを含み得る。その後顧客は、各ファイルについて所望のセキュリティ・レベルを指定し（ステップ５４）、セキュリティ情報を含むテーブルを作成する（ステップ５６）。

【００３０】その後顧客は、暗号化されたソフトウエアが書き込まれるべきプログラム可能なＣＤ－ＲＯＭディスクに関する予め形成されたＩＤ２２および固有のＩＤ

２４に対応する情報を入力する。他の実施例にあっては、これらの値は、それらが記録される任意の場所からプログラム可能なＣＤ－ＲＯＭから読み出される。セキュリティ・ソフトウエアが予め形成されたＩＤ２２および固有のＩＤ２４を取得すると、ステップ６２において、それらを共に利用して暗号キーを作成する。暗号化プログラム６３は、ステップ６４においてその暗号キーを利用し、実行可能なファイルおよびセキュリティ・レベル・テーブルを暗号化する。ステップ６４で暗号化されたファイルは、その後ステップ７０においてラッパ(wrapper)プログラムにデータ・ファイルとして付加される。ラッパ・プログラムは、セキュリティ・テーブルにおける指定によって許容されるようなディスク１０からの予め形成されたＩＤ２２および固有のＩＤ２４を読み込むのに必要なサブルーチンと、プログラムが走っているコンピュータのメモリ内にリバース・エンジニアリング・ツールが存在することを検出し、それらが検出された場合には実行を中断させるサブルーチンと、ソフトウエア・アプリケーションの暗号化解除および実行を開始するサブルーチンとを含む。ステップ７２において、ラップされた実行可能パッケージは、書き込み可能セッション（１６または１８）においてプログラム可能なＣＤ－ＲＯＭディスクに書き込まれる。

【００３１】暗号作成法および暗号化機能は当該技術分野で周知である。これに関し、Applied Cryptography, B.Schneier, John Wiley and Sons, Inc., New York, 1996に適切な記載があり、この内容は本願でも使用可能である。本実施例では、以下の表記方法を採用する：

表１

暗号化標記

記号	意味
P	暗号化されるべきプログラム
E	暗号化関数
B	予め形成されたＩＤ
U	固有のＩＤ
I	連結したＩＤ＝ＢＵ
X	暗号化されたプログラム＝Ｅ（Ｐ，Ｉ）

本発明に関し、以下の条件を満足する任意の暗号化関数が利用可能であり、それは：Ｅ（Ｐ，Ｉ）の計算が実行可能に適切であること，すなわちＥが多項式タイム(polynomial time)で計算可能であること；E^{-1}（Ｘ，Ｉ）の計算に関する多項式タイム・アルゴリズムが既知であって実行可能に適切であること；暗号化関数Ｅ（およびその解読に相当するE^{-1}）が、その計算の際に提供される可変なキーＩを利用すること；および暗号化／暗号解除プロセスを通じて良好でないプログラムＰ’（$P'=E^{-1}\{E(P,I),I\}$）を形成してしまう蓋然性が非常に小さいこと、である。

【００３２】暗号化のステップは以下のとおりである：

１．予め形成されたＩＤ　Ｂおよび固有のＩＤ　Ｕを取得する；

２．２つのＩＤが連結され（Ｉ＝ＢＵ）、暗号化／暗号化解除キーＩを求める；

３．暗号化アルゴリズムＥで連結されたＩＤが使用され、暗号化されたプログラムＸ＝Ｅ（Ｐ，Ｉ）を計算する；

暗号化解除のステップは以下のとおりである：

１．予め形成されたＩＤ　Ｂおよび固有のＩＤ　Ｂを取得する；

２．２つのＩＤが連結され（Ｉ＝ＢＵ）、暗号化／暗号化解除キーＩを求める；

３．暗号化解除アルゴリズムE^{-1}で連結されたＩＤが使用され、当初のプログラム$P=E^{-1}$（Ｘ，Ｉ）を計算する；

図４を参照するに、本発明の第１実施例に関するブロック図が示される。マスタ・コンパクト・ディスクに関する周知のマスタ技術を利用して、プログラム可能なＣＤ－ＲＯＭディスクがマスタされる（ステップ８０）。プログラム可能なＣＤ－ＲＯＭは第１セッション１４を含むが、それに加えて他のマスタ・セッションを含むことも可能である。マスタ・ディスクに含まれるものは、予め形成されたＩＤ２２である。その後ステップ８２において、マスタ・ディスクを利用して、標準的なスタンプ(stamp)手法によりプログラム可能なＣＤ－ＲＯＭディスクを製造する。この時点では、多数の同一のプログラム可能なＣＤ－ＲＯＭディスクが存在する。

【００３３】その後ディスク１０は各自の識別子を利用して書き込まれる。ステップ８４において、固有のＩＤ２４が形成される。固有のＩＤ２４は、ディスク１０の製造順によって定められるところの連続的に定められた番号とすることが可能であり、完全にランダムな番号とすることも可能であり、または予め形成された番号のテーブルから選択することも可能である。他の好適な実施例では、その番号はアルゴリズムによって更に処理され、そのアルゴリズムは、有効な番号(valid number)はとり得る番号の範囲内の小さな部分にのみ対応しているように使用番号(actual number)を生成可能である。この場合、有効な番号は、そのような生成アルゴリズムを知ることによってのみ作成可能である。また、この場合は、検査アルゴリズムを提供し、例えば周知の公開キー，プライベート・キー暗号化および署名の手法を利用することによって、番号を認めることも可能である。他の実施例では、その番号はハードウエア身元確認により生成され、特定のコンピュータに関連付けられる。（この点については、例えばO’Connor et al., U.S. 5,745,568があり、本願でも使用可能である。）他の実施例では、固有のＩＤ２４が特定のアプリケーションに関連付けられ、このため同一の固有の識別番号が複数のディスク１０上で使用される。固有のＩＤ２４は、書き込み済みセッションとなるＩＳＯ９６６０両立可能ファイル

・イメージを作成するために使用される（ステップ８６）。このセッションの既知の絶対セクタ・アドレスに関する主チャネル・データは、固有のＩＤ２４を利用して修正され（ステップ８８）、ステップ９０において第２セッション１６としてディスク１０に加圧されずに書き込まれる。なお、このセッションは第３またはそれ以降のセッションとして書き込まれることも可能である。この時点において、各ディスク１０は、各自自身の識別子を包含し、特有のものとなる。

【００３４】顧客は暗号化に備えてディスク１０を用意する。この段階は、ステップ７４として図示され、図３で詳細に説明したセキュリティ・ソフトウエアによって実行される複数のステップより成る。固有のＩＤ２４は、第２セッション１６における既知の絶対セクタ・アドレスから読み取られる（ステップ９２）。暗号化は、ステップ７６として図示され、図３で詳細に説明した多数のステップより成る。暗号化が完了すると、ディスク１０上の第３セッション１８にラップされた実行可能なものが書き込まれる（ステップ９４）。

【００３５】図５を参照するに、本発明の第２実施例のブロック図が示され、固有のＩＤ２４および暗号化された実行可能なもの４０が同じセッションに書き込まれている。これは、図４で説明したものと同じステップをいくつか含んでいるが、その順序が異なる。プログラム可能なＣＤ－ＲＯＭディスクは、マスタ・コンパクト・ディスクに関して周知のマスタ技術を利用してマスタされる（ステップ８０）。プログラム可能なＣＤ－ＲＯＭは第１セッション１４を含むが、さらに他のマスタ・セッションを含むことも可能である。ディスク１０に含まれているものは予め形成されたＩＤ２２である。その後ステップ８２において、マスタ・ディスクを利用して、標準的なスタンプ手法によりプログラム可能なＣＤ－ＲＯＭディスクを製造する。この時点では、多数の同一のプログラム可能なＣＤ－ＲＯＭディスクが存在する。

【００３６】顧客は暗号化に備えてディスク１０を用意する。この段階は、ステップ７４として図示され、図３で詳細に説明したセキュリティ・ソフトウエアによって実行される複数のステップより成る。固有のＩＤ２４がステップ８４で形成される。固有のＩＤ２４は完全にランダムな番号とすることが可能であり、予め形成された番号のテーブルから選択することも可能である。固有のＩＤ２４は、書き込み済みセッションとなるＩＳＯ９６６０両立可能ファイル・イメージを作成するために使用される（ステップ８６）。このセッションの既知の絶対セクタ・アドレスに関する主チャネル・データは、固有のＩＤ２４を利用して修正される（ステップ８８）。ステップ７４で読み込んだ予め形成されたＩＤ２２と共に、固有のＩＤ２４を利用して、暗号化を行う。暗号化は、ステップ７６として図示され、図３で詳細に説明した多数のステップより成る。暗号化が完了すると、ディスク１０上の第３セッション１８にラップされた実行可能なものが書き込まれる。

【００３７】図６を参照するに、本発明によるエンド・ユーザで実行するための方法が示される。まず、エンド・ユーザはディスク１０をＣＤ－ＲＯＭ，ＣＤ－ＲまたはＣＤ－ＲＷドライブにディスク１０を挿入する（ステップ１００）。ディスク１０上で実行可能なプログラムが自動的に走り出しまたは選択される（ステップ１０２）。プログラムは先ず対ハッキング(anti-hacking)サブルーチン３４を使用して、ハッキングまたはコピー・プロテクト対策を打ち破るために使用され得るカーネル・デバッグ・ソフトウエア(kernel-debugging software)の検査を行う（ステップ１０４）。そのようなプログラムが存在すると、そのプログラムはユーザにエラー・メッセージを示し、自動的に停止する（ステップ１０６）。

【００３８】そのようなハッキング・ソフトウエアがエンド・ユーザのシステムに存在しない場合は、ステップ１０８において暗号化解除プログラムがドライブＩＤを読み出す。ステップ１１０において、暗号化解除プログラムは、そのドライブに対して、ＡＴＩＰ信号から予め形成されたＩＤ２２を読み出すための命令を発行する。暗号化解除プログラムは、そのドライブに対して、サブ・コードから予め形成されたＩＤ２２を読み出すための命令を発行する（ステップ１１２）。ステップ１１４において、暗号化解除プログラムは、主データ・チャネルの既知の絶対セクタ・アドレスから予め形成されたＩＤ２２を読み出すための命令を発行する。そして、ステップ１１６において、暗号化解除プログラムは、そのドライブに対して、第２の（後続の）セッションの主データ・チャネルの既知の絶対セクタ・アドレスから固有のＩＤ２４を読み出すための命令を発行する。

【００３９】ステップ１１８において、暗号化解除プログラムは、ステップ１１６で読み込んだ固有のＩＤ２４と、ステップ１１０でＡＴＩＰから読み込んだ予め形成されたＩＤ２２とを連結する。ステップ１２０において、その連結された結果を暗号化解除キーとして利用して、ラップされたソフトウエア３２の暗号化を解除する。ステップ１２２において、プログラムは、その暗号化解除が有効であるか否かを判定する。これを行ういくつかの手法が存在し、例えば、暗号化解除されたプログラム内のフラグを探索したり、オペレーティング・システム固有のコードが暗号化解除された実行可能なものの中に存在するか否かを検査することが可能である。暗号化解除が成功すると、当初の実行可能なものが開始される（ステップ１２４）。

【００４０】暗号化解除に失敗すると、暗号化解除プログラムは、ステップ１０８で読み出したドライブＩＤを利用して、そのドライブがＡＴＩＰを読み出し得るべきか否かを判定する（ステップ１２６）。ドライブがＡＴ

ＩＰ包含リストにあれば（そのドライブがＡＴＩＰを読み出し得るべきであれば）、プログラムはユーザにエラー・メッセージを示し、停止する（ステップ１０６）。ドライブがＡＴＩＰ包含リストになければ、暗号化解除プログラムは、ステップ５６で記録したセキュリティ・テーブルを参照する（ステップ１２８）。プログラムのセキュリティ・レベルが最高レベルに設定されていた場合は、サブコードにおける予め形成されたＩＤ２２を使用することは認められず、プログラムはユーザにエラー・メッセージを示し、停止する（ステップ１０６）。サブコードからの予め形成されたＩＤ２２が許容される場合は、暗号化解除プログラムは、ステップ１１６で読み出した固有のＩＤ２４と、ステップ１１２でサブコードから読み出した予め形成されたＩＤ２２とを連結させる（ステップ１３０）。そして、ステップ１３２においてラップされたソフトウエア３２の暗号化を解除する暗号化解除キーとして、その連結された結果物を使用する。その後プログラムは暗号化解除が有効であるか否かを判定する（ステップ１３４）。暗号化解除が成功すると、当初の実行可能なものが開始される（ステップ１２４）。

【００４１】暗号化解除に失敗すると、暗号化解除プログラムは、ステップ１０８で読み出したドライブＩＤを利用して、そのドライブがサブコードを読み出し得るべきか否かを判定する（ステップ１３６）。ドライブがサブコード包含リストにあれば（それがサブコードを読み出し得るべきであれば）、プログラムはユーザにエラー・メッセージを示し、停止する（ステップ１０６）。ドライブがサブコード包含リストになければ、暗号化解除プログラムは、ステップ５６で記録したセキュリティ・テーブルを参照する（ステップ１３８）。プログラムのセキュリティ・レベルが高いレベルに設定されていた場合は、主データにおける予め形成されたＩＤ２２を使用することは認められず、プログラムはユーザにエラー・メッセージを示し、停止する（ステップ１０６）。主データからの予め形成されたＩＤ２２が許容される場合は、暗号化解除プログラムは、ステップ１１６で読み出した固有のＩＤ２４と、ステップ１１４で主データから読み出した予め形成されたＩＤ２２とを連結させる（ステップ１４０）。そして、ステップ１４２においてラップされたソフトウエア３２の暗号化を解除する暗号化解除キーとして、その連結された結果物を使用する。その後プログラムは暗号化解除が有効であるか否かを判定する（ステップ１４４）。暗号化解除が成功すると、当初の実行可能なものが開始される（ステップ１２４）。暗号化解除に失敗すると、エラー・メッセージがユーザに示され、プログラムーおよび全プロセスーが終了する（ステップ１０６）。

【００４２】暗号化解除が成功する任意の時点において（ステップ１２２，１３４，１４４）、当初の実行可能なものが開始される（ステップ１２４）。暗号化解除プログラムは背景に残り（ステップ１４８）、プログラムは実行され（ステップ１４６）および抜け出す（ステップ１５０）。当初のプログラムが抜け出ると、暗号化解除プログラムは、メモリおよび当初プログラムの使用したハード・ドライブの領域をクリアし（ステップ１５２）、終了する（ステップ１５４）。

【図面の簡単な説明】

【図１】図１は、本発明によるコピー・プロテクトを有するコンパクト・ディスクの平面図である。

【図２】図２は、コピー不可能にアプリケーションを暗号化するソフトウエア手法の概略図である。

【図３】図３は、暗号化されたソフトウエアを形成するためのステップを示すブロック図である。

【図４】図４は、コピー・プロテクトがＣＤにどのように提供されるかの一例を示すブロック図である。

【図５】図５は、コピー・プロテクトがＣＤにどのように提供されるかの他の例を示すブロック図である。

【図６】図６は、ＣＤが読み込まれる場合に、コピー・プロテクトがどのように機能するかを示すブロック図である。

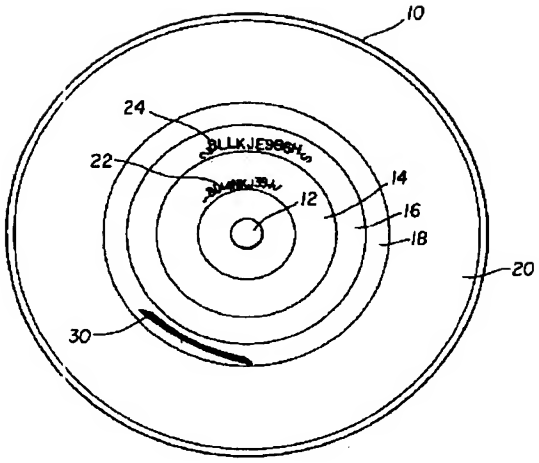
【図７】図７は、ここに開示したコピー・プロテクトが、それを破ろうとする方法をどのようにして阻止するかを示すブロック図である。

【符号の説明】

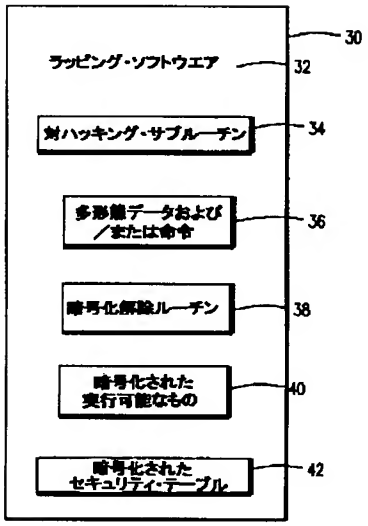
１０　光学ディスク
１４　第１セッション
１６　第２セッション
１８　第３セッション
２０　再記録可能な領域
２２　予め形成されたＩＤ
２４　固有のＩＤ
３０　パッケージ

【図６】

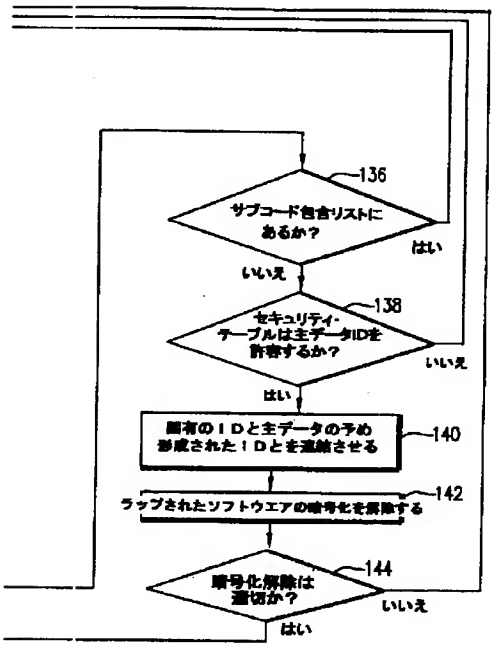
【図１】


10
24
22
14
12
16
18
20
30

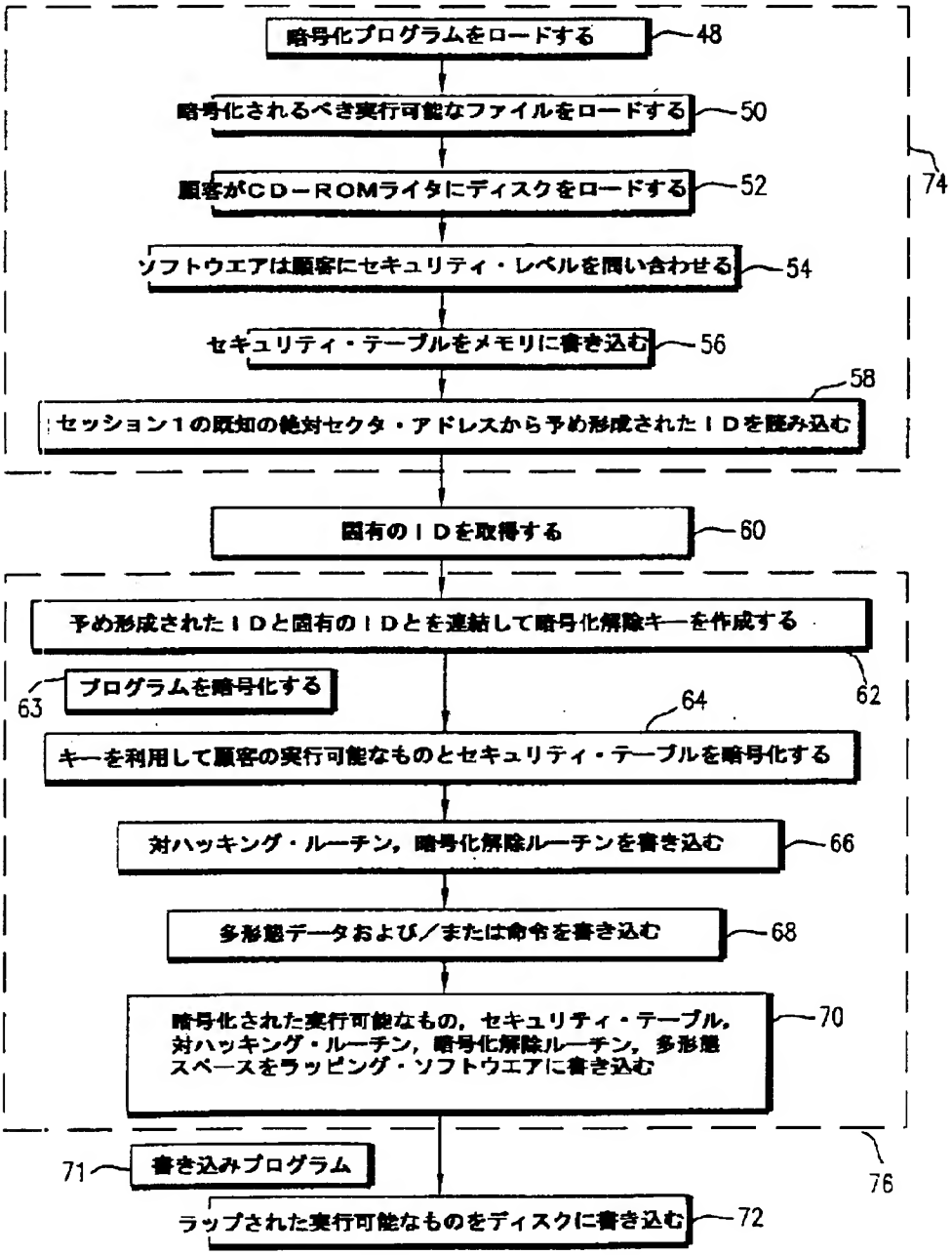
【図２】


30
ラッピング・ソフトウエア
32
対ハッキング・サブルーチン
34
多形態データおよび／または命令
36
暗号化解除ルーチン
38
暗号化された実行可能なもの
40
暗号化されたセキュリティ・テーブル
42

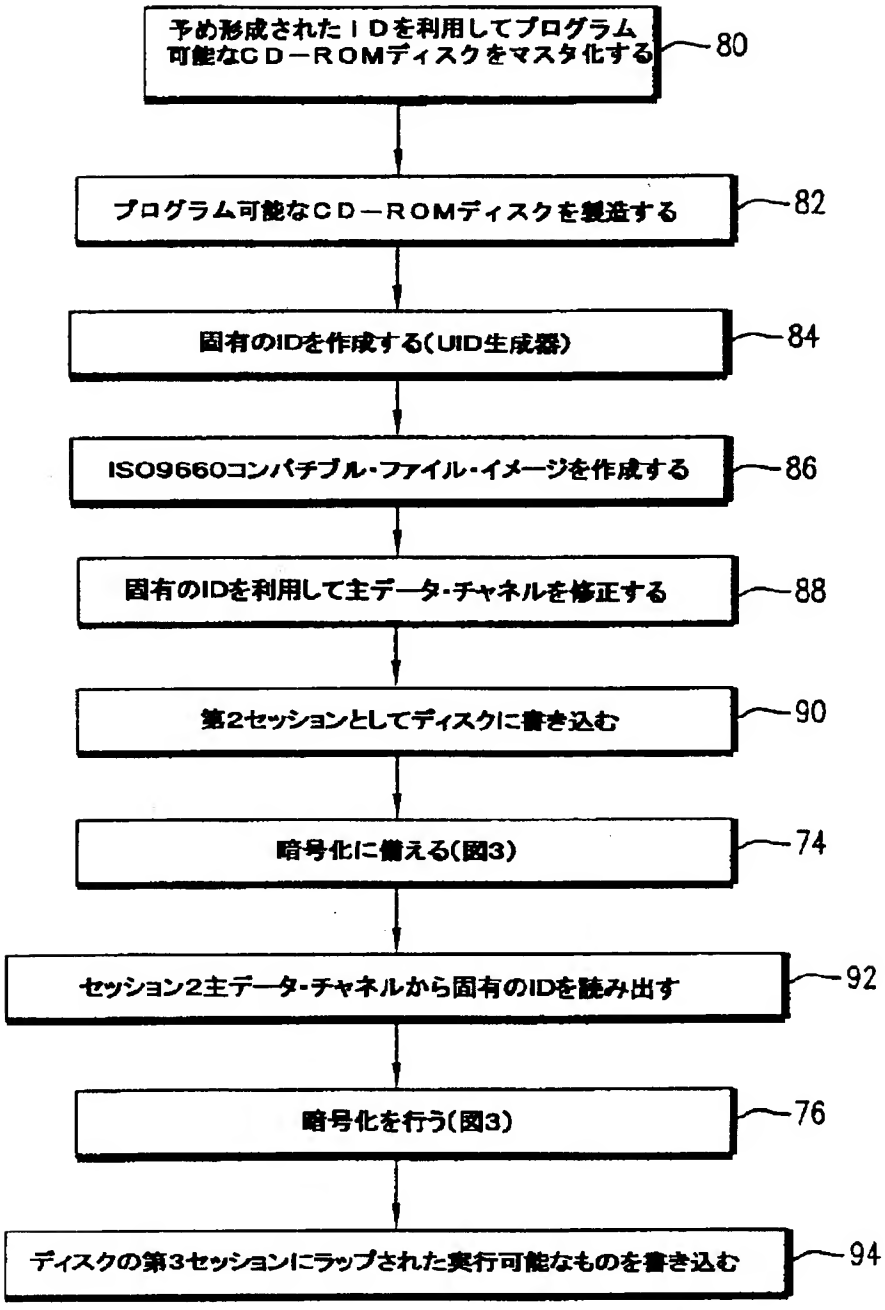
【図６Ｂ】


136
サブコード包含リストにあるか？
はい
いいえ
138
セキュリティ・テーブルは主データIDを許容するか？
いいえ
はい
固有のＩＤと主データの予め形成されたＩＤとを連結させる
140
ラップされたソフトウエアの暗号化を解除する
142
144
暗号化解除は適切か？
いいえ
はい

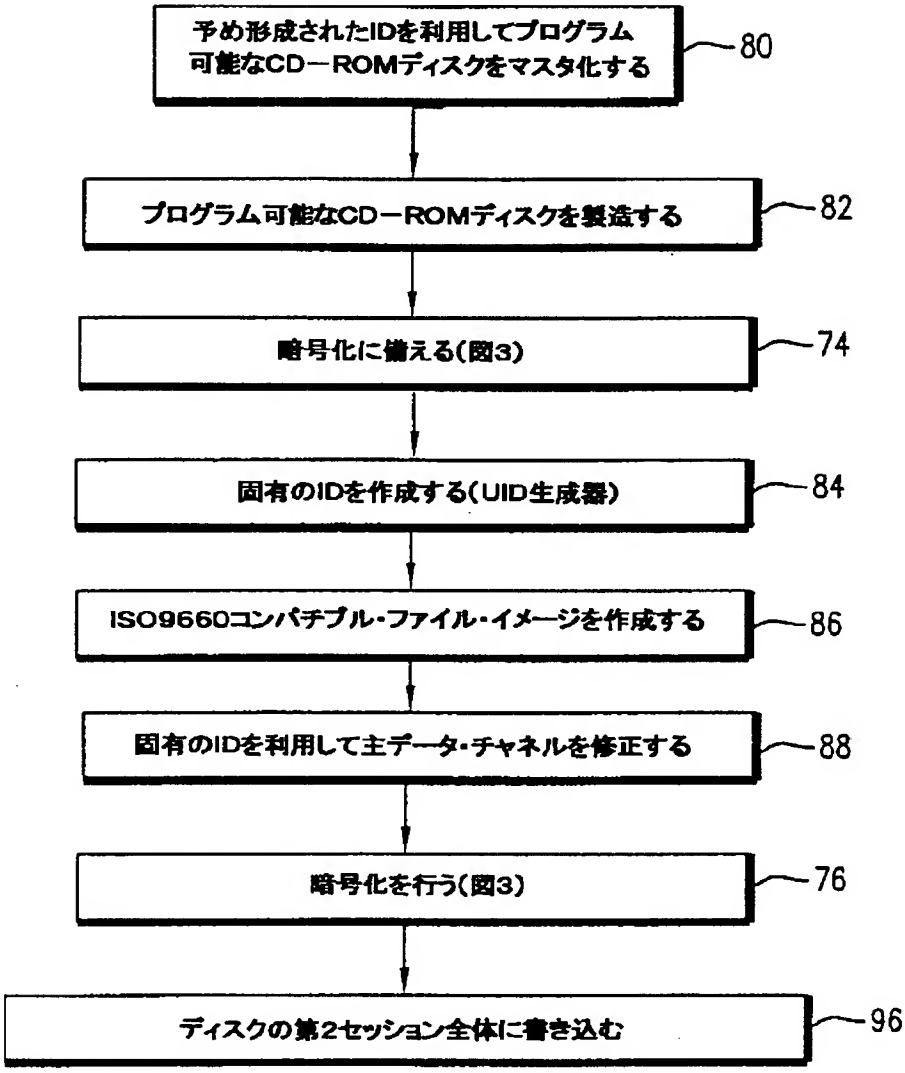
【図３】


暗号化プログラムをロードする
48
暗号化されるべき実行可能なファイルをロードする
50
顧客がCD－ROMライタにディスクをロードする
52
74
ソフトウエアは顧客にセキュリティ・レベルを問い合わせる
54
セキュリティ・テーブルをメモリに書き込む
56
58
セッション１の既知の絶対セクタ・アドレスから予め形成されたＩＤを読み込む
固有のＩＤを取得する
60
予め形成されたＩＤと固有のＩＤとを連結して暗号化解除キーを作成する
62
63
プログラムを暗号化する
64
キーを利用して顧客の実行可能なものとセキュリティ・テーブルを暗号化する
対ハッキング・ルーチン，暗号化解除ルーチンを書き込む
66
多形態データおよび／または命令を書き込む
68
暗号化された実行可能なもの，セキュリティ・テーブル，
対ハッキング・ルーチン，暗号化解除ルーチン，多形態
スペースをラッピング・ソフトウエアに書き込む
70
76
71
書き込みプログラム
ラップされた実行可能なものをディスクに書き込む
72

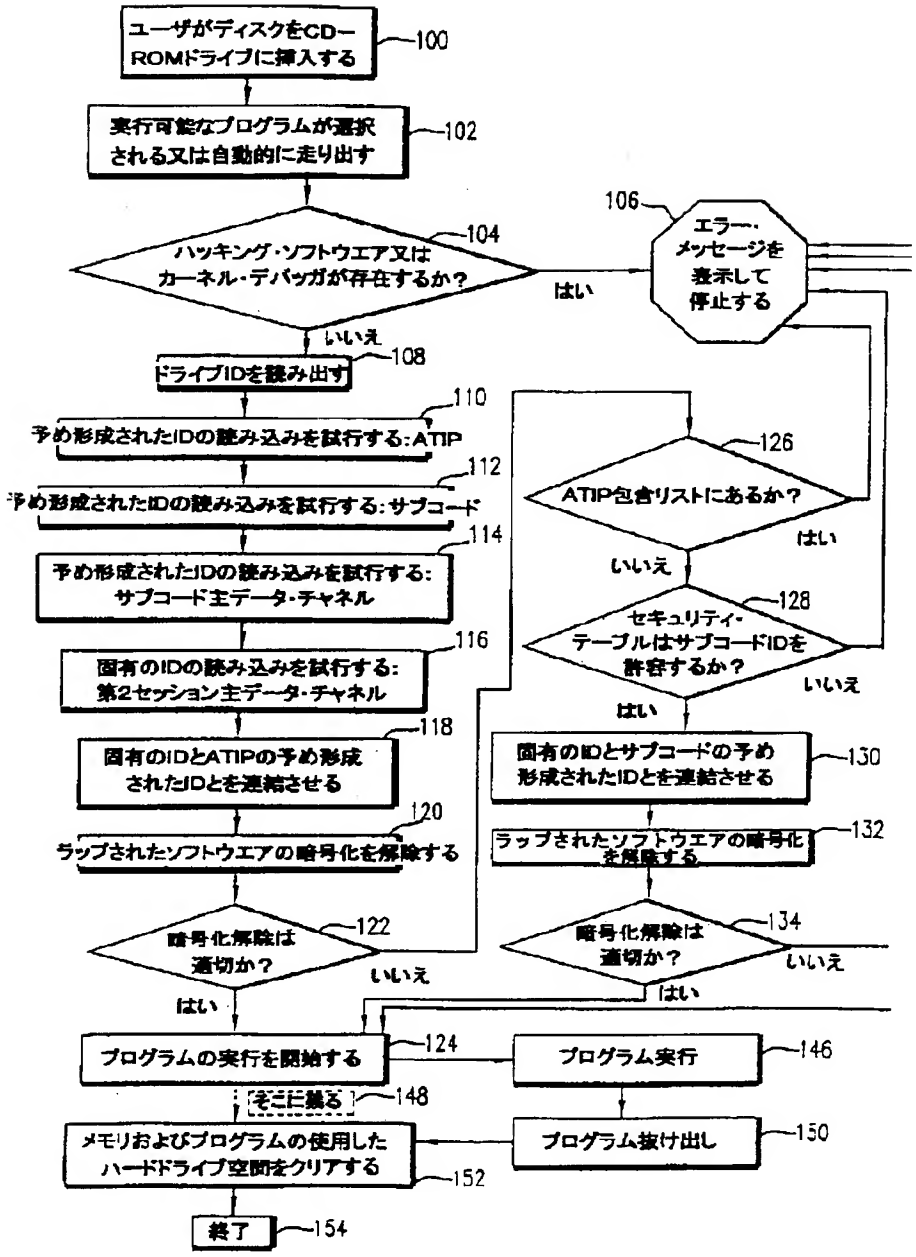
【図４】


予め形成されたＩＤを利用してプログラム可能なＣＤ－ＲＯＭディスクをマスタ化する
80
プログラム可能なＣＤ－ＲＯＭディスクを製造する
82
固有のIDを作成する(UID生成器)
84
ISO9660コンパチブル・ファイル・イメージを作成する
86
固有のIDを利用して主データ・チャネルを修正する
88
第2セッションとしてディスクに書き込む
90
暗号化に備える(図3)
74
セッション2主データ・チャネルから固有のIDを読み出す
92
暗号化を行う(図3)
76
ディスクの第3セッションにラップされた実行可能なものを書き込む
94

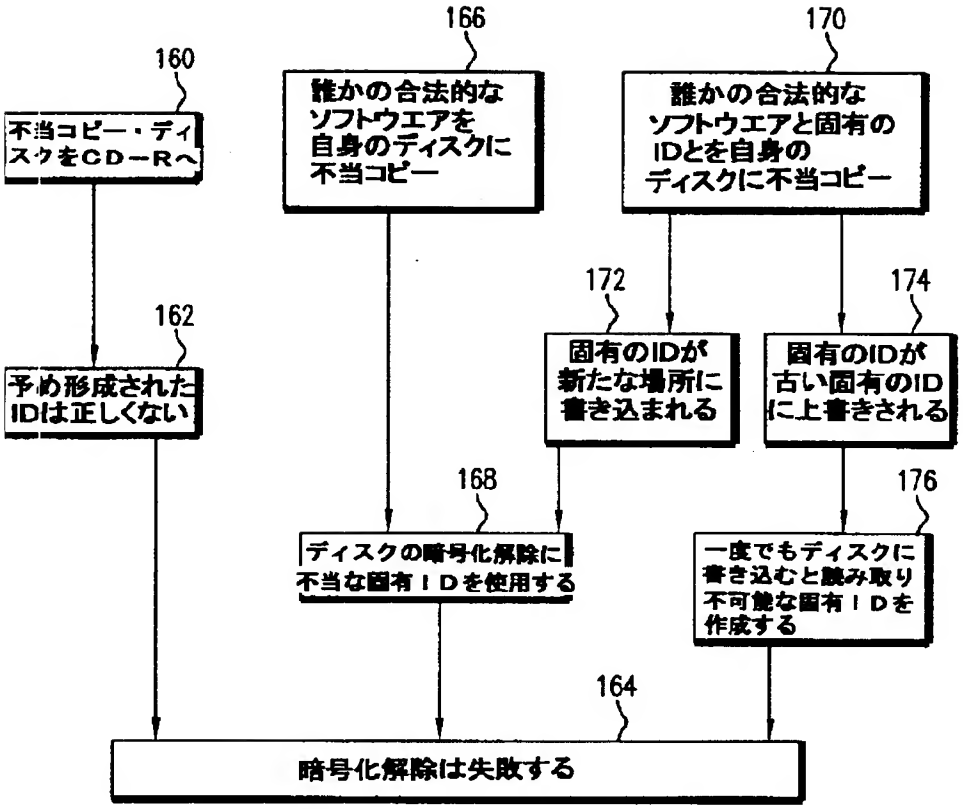
【図５】


予め形成されたIDを利用してプログラム可能なCD－ROMディスクをマスタ化する
80
プログラム可能なCD－ROMディスクを製造する
82
暗号化に備える(図3)
74
固有のIDを作成する(UID生成器)
84
ISO9660コンパチブル・ファイル・イメージを作成する
86
固有のIDを利用して主データ・チャネルを修正する
88
暗号化を行う(図3)
76
ディスクの第2セッション全体に書き込む
96

【図６Ａ】


ユーザがディスクをCD-ROMドライブに挿入する
100
実行可能なプログラムが選択される又は自動的に走り出す
102
ハッキング・ソフトウエア又はカーネル・デバッガが存在するか？
104
はい
106
エラー・メッセージを表示して停止する
いいえ
ドライブIDを読み出す
108
予め形成されたIDの読み込みを試行する：ATIP
110
予め形成されたIDの読み込みを試行する：サブコード
112
予め形成されたIDの読み込みを試行する：サブコード主データ・チャネル
114
固有のIDの読み込みを試行する：第2セッション主データ・チャネル
116
固有のIDとATIPの予め形成されたIDとを連結させる
118
ラップされたソフトウエアの暗号化を解除する
120
暗号化解除は適切か？
122
いいえ
はい
ATIP包含リストにあるか？
126
はい
いいえ
セキュリティ・テーブルはサブコードIDを許容するか？
128
いいえ
はい
固有のIDとサブコードの予め形成されたIDとを連結させる
130
ラップされたソフトウエアの暗号化を解除する
132
暗号化解除は適切か？
134
いいえ
はい
プログラムの実行を開始する
124
プログラム実行
146
そこに戻る
148
メモリおよびプログラムの使用したハードドライブ空間をクリアする
152
プログラム抜け出し
150
終了
154

【図７】



フロントページの続き

(51) Int. Cl.[7]	識別記号	Ｆ Ｉ	ﾃｰﾏｺｰﾄﾞ（参考）
Ｇ１１Ｂ 7/007		Ｇ１１Ｂ 20/12	
20/12		Ｇ０６Ｆ 9/06	６６０Ｇ

(72)発明者 ブルース エル ハ
アメリカ合衆国 ニューヨーク 14580
ウェブスター レイク・ロード 1072

Ｆターム(参考) 5B017 AA06 AA07 BA07 CA09 CA15
5B076 FA05 FC06
5D044 BC04 CC04 DE49 DE50 DE54
DE55 GK17
5D090 AA01 BB04 CC12 CC14 FF09
GG03 GG32 HH01